(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : 2 792 143

(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : 99 04537

(51) Int Cl[7] : H 04 L 9/32, H 04 M 11/00, H 04 Q 7/32, G 06 K 19/07

(12) DEMANDE DE BREVET D'INVENTION A1

(22) Date de dépôt : 12.04.99.

(30) Priorité :

(43) Date de mise à la disposition du public de la demande : 13.10.00 Bulletin 00/41.

(56) Liste des documents cités dans le rapport de recherche préliminaire : *Se reporter à la fin du présent fascicule*

(60) Références à d'autres documents nationaux apparentés :

(71) Demandeur(s) : *SARL SMART DESIGN Société à responsabilité limitée* — FR.

(72) Inventeur(s) : EONNET YVES.

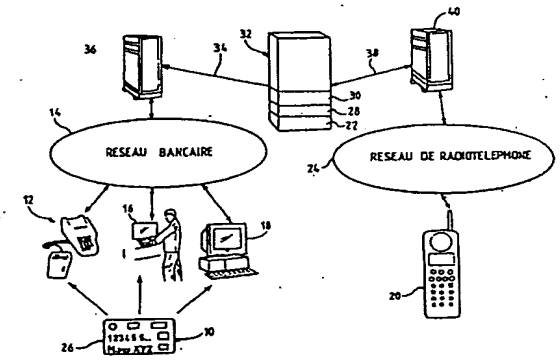
(73) Titulaire(s) :

(74) Mandataire(s) : ERNEST GUTMANN YVES PLASSERAUD SA.

(54) PROCEDE ET SYSTEME DE SECURISATION DE L'UTILISATION DE CARTES COMPORTANT DES MOYENS D'IDENTIFICATION ET/OU D'AUTHENTIFICATION.

(57) Procédé et système de sécurisation de l'utilisation de cartes (10) comportant des moyens d'identification et/ ou d'authentification, telles que des cartes bancaires de paiement, par association de chaque carte (10) à un radiotéléphone (20), localisation du radiotéléphone (20) à chaque utilisation de la carte (10) sur un terminal de paiement (12, 16, 18), validation de l'utilisation de la carte (10) si les emplacements du terminal (12, 16, 18) et du radiotéléphone (20) correspondent et appel du radiotéléphone (20) dans le cas contraire pour demander l'acceptation ou le refus par le porteur du radiotéléphone de l'utilisation précitée de la carte (10).

L'invention s'applique notamment à la sécurisation de l'utilisation des cartes bancaires de paiement et de toutes autres cartes ou (supports d'informations comprenant des) moyens d'identification ou d'authentification.



FR 2 792 143 - A1

L'invention concerne un procédé et un système de sécurisation de l'utilisation de cartes et autres (supports comportant des) moyens d'identification et/ou d'authentification, en particulier de cartes bancaires de paiement.

Les cartes de paiement à bande magnétique ou à circuit intégré, sont actuellement fournies par des banques ou établissements analogues à leurs clients, éventuellement avec des codes confidentiels qu'il faut entrer sur les terminaux informatiques avec lesquels ces cartes sont utilisées, pour effectuer des paiements, retirer des billets de banque, etc...

Il peut cependant arriver qu'une carte perdue ou volée soit utilisée par un tiers, sans que le détenteur de la carte soit informé de cette utilisation et sans qu'il puisse s'y opposer (sur le réseau internet par exemple).

Il peut également arriver que le détenteur d'une carte de paiement la prête à une autre personne en lui communiquant le code confidentiel pour qu'elle puisse l'utiliser sur un terminal informatique. Le détenteur de la carte n'est alors informé qu'ultérieurement des paiements effectués avec sa carte, à réception d'un relevé de compte bancaire ou après interrogation de la banque qui lui a fourni la carte de paiement.

De telles cartes sont aussi utilisables, mais sans sécurité d'identification ou d'authentification, pour effectuer des paiements à distance, notamment sur le réseau Internet ou par téléphone.

Il existe d'autres cartes ou moyens d'identification ou d'authentification, sur supports d'information comme par exemple que des cartes de santé, des porte-monnaies électroniques, des cartes d'accès à des installations protégées, etc. ou sans support, tels que par exemple des codes confidentiels d'accès, etc., qui sont utilisables avec ou sans code confidentiel sur des terminaux informatiques, et dont les détenteurs n'ont aucun moyen d'être informés d'une éventuelle utilisation frauduleuse ou non conforme par des tiers.

L'invention a pour but d'apporter une solution simple et efficace à ce problème.

Elle a pour objet un procédé et un système de sécurisation de l'utilisation des cartes précitées, permettant à leurs détenteurs d'être informés de leur utilisation par des tiers et de s'opposer éventuellement à cette utilisation.

Elle a également pour objet un procédé et un système du type précité, qui mettent en œuvre des moyens et des réseaux de communication préexistants et qui ne nécessitent donc pas un investissement trop onéreux.

Elle propose, à cet effet, un procédé de sécurisation de l'utilisation de cartes et autres (supports comportant des) moyens d'identification et/ou d'authentification, en particulier de cartes bancaires de paiement, caractérisé en ce qu'il consiste :

- à associer chaque carte à un téléphone mobile équipé d'un moyen (par exemple d'un module) d'identification d'abonné à circuits intégrés (ou autres) et à enregistrer dans une base de données un couple d'informations comprenant un identifiant de la carte de paiement et un identifiant du téléphone mobile ou de l'abonné, et

- à chaque utilisation de la carte précitée sur un terminal informatique dont l'emplacement est connu, à localiser au moyen du réseau radiotéléphonique le téléphone mobile associé à cette carte, à comparer l'emplacement du terminal informatique et l'emplacement localisé du téléphone mobile et, en fonction du résultat de cette comparaison, à valider l'utilisation de la carte sur le terminal informatique ou à appeler le téléphone mobile pour acceptation ou refus par son porteur de l'utilisation de la carte sur ledit terminal informatique.

L'invention tire parti des caractéristiques des réseaux de radiotéléphonie du type GSM ou autres, qui consistent à connaître en permanence (ou presque) la localisation d'un téléphone mobile par rapport à un réseau cellulaire de stations de base avec lesquelles les téléphones mobiles communiquent par liaison radio. Cette localisation d'un téléphone mobile est relativement précise, au moins dans les zones urbaines, et l'invention est basée sur le fait qu'une concordance entre l'emplacement localisé d'un téléphone mobile et l'emplacement d'un terminal informatique sur lequel est utilisée une carte de paiement associée à ce téléphone mobile, permet de supposer, au moins dans

une certaine mesure, que la carte de paiement est utilisée par le porteur du téléphone mobile.

Dans le cas où l'emplacement localisé du téléphone mobile ne concorde pas avec l'emplacement du terminal informatique utilisé, l'invention prévoit d'appeler le téléphone mobile pour demander à son porteur d'accepter ou de refuser l'utilisation de sa carte sur le terminal informatique précité.

Le porteur du téléphone mobile validera cette utilisation s'il a lui-même utilisé la carte et pourra soit accepter cette utilisation, soit la refuser s'il n'a pas lui-même utilisé la carte, celle-ci pouvant être confiée à une tierce personne, ou perdue ou volée.

Selon une autre caractéristique de l'invention, ce procédé consiste également, à la première utilisation d'un terminal informatique au moyen d'une carte précitée, à enregistrer un identifiant de ce terminal et son emplacement déterminé par la localisation du téléphone mobile associé à la carte, et à constituer une base de données contenant les identifiants et les emplacements des terminaux informatiques utilisés au moyen des cartes précitées.

Lors d'une utilisation ultérieure du même terminal, par exemple avec une autre carte, le procédé consiste à déterminer l'emplacement du terminal par localisation du téléphone mobile associé à cette autre carte, à vérifier la concordance entre cet emplacement et celui enregistré précédemment dans la base de données et, en cas de discordance entre ces emplacements, à appeler le téléphone mobile pour acceptation ou refus de l'utilisation de ladite autre carte sur ce terminal.

Selon encore une autre caractéristique de l'invention, ce procédé consiste à enregistrer dans les circuits intégrés du moyen (notamment du module) d'identification d'abonné équipant le téléphone mobile, un logiciel comprenant des moyens d'authentification de la carte de paiement associée au téléphone mobile. Cela permet notamment, quand la localisation du téléphone mobile coïncide avec l'emplacement du terminal informatique et qu'une transaction effectuée avec la carte sur ce terminal est acceptée, de faire produire par le moyen (module) précité du téléphone mobile un certificat de transaction.

L'invention prévoit également d'enregistrer dans les circuits intégrés du moyen (module) d'identification d'abonné un logiciel comprenant des fonctions d'autorisation préalable d'au moins une utilisation prévue de la carte associée, d'activation et de désactivation de cette carte, et d'acceptation et de refus d'une utilisation de ladite carte.

L'exécution de ces fonctions peut être commandée de façon simple et rapide par le porteur du téléphone mobile, grâce aux touches de fonctions du clavier de son téléphone.

Selon encore une autre caractéristique de l'invention, ce procédé consiste à associer au moins deux cartes précitées à un téléphone mobile équipé d'un moyen (en particulier d'un module) d'identification d'abonné, l'une de ces cartes étant utilisable par le porteur du téléphone mobile et l'autre par une autre personne, et à soumettre chaque utilisation de ladite autre carte à une autorisation préalable, à une acceptation ou à un refus par le porteur du téléphone mobile.

Cela permet notamment à une personne de conserver sa propre carte et de contrôler en permanence l'utilisation d'une autre carte qu'elle a confiée à un tiers.

Les informations associées aux cartes précitées et concernant leur nature, leur état d'activation ou de désactivation, les conditions limites de leur utilisation et les autorisations préalables d'utilisation sont avantageusement enregistrées dans une base de données pour pouvoir être utilisées à tout moment approprié.

L'invention propose également un système de sécurisation de l'utilisation de cartes et autres (supports comportant des) moyens d'identification et/ou d'authentification, en particulier de cartes bancaires de paiement, caractérisé en ce qu'il comprend :

- une première base de données dans laquelle sont enregistrés des identifiants de téléphones mobiles ou de leurs abonnés et des identifiants de cartes précitées qui sont détenues par les abonnés ou par des personnes autorisées par les abonnés, chaque identifiant de carte étant associé à un identifiant de téléphone mobile ou d'abonné,

- une deuxième base de données dans laquelle sont enregistrés des identifiants et des emplacements de terminaux informatiques sur lesquels les cartes précitées sont utilisables,

- des moyens de traitement de l'information pour la constitution, la mise à jour et la gestion desdites bases de données,

- des moyens de connexion de ces moyens de traitement de l'information à un serveur d'un système existant de traitement de l'utilisation des cartes précitées sur des terminaux informatiques et à un serveur d'un réseau de radiotéléphonie sur lequel les téléphones mobiles précités sont utilisables,

- lesdits moyens de traitement de l'information étant conçus pour, à chaque utilisation d'une carte précitée sur un terminal informatique, trouver dans la première base de données l'identifiant de téléphone mobile ou d'abonné qui est associé à l'identifiant de la carte utilisée, transmettre au serveur du réseau de radiotéléphonie une demande de localisation du téléphone mobile associé à ladite carte, trouver dans la deuxième base de données l'emplacement du terminal informatique utilisé par ladite carte, comparer cet emplacement avec l'emplacement localisé du téléphone mobile et, en fonction des résultats de cette comparaison, accepter l'utilisation de la carte sur le terminal ou envoyer un message au téléphone mobile demandant une acceptation ou un refus de l'utilisation de la carte par le porteur du téléphone mobile.

Selon d'autres caractéristiques de l'invention,

- l'identifiant d'une carte associée à un téléphone mobile permet de la distinguer d'une carte non associée à un téléphone mobile,

- le moyen (module) d'identification d'abonné équipant le téléphone mobile comprend des moyens d'authentification de la carte associée, des moyens d'autorisation préalable d'au moins une utilisation prévue de cette carte, des moyens d'activation et de désactivation de cette carte, et des moyens d'acceptation ou de refus d'une utilisation de cette carte sur un terminal informatique,

- au moins une deuxième carte est associée à un téléphone mobile déjà associé à une première carte et est utilisable par une autre personne que le

porteur du téléphone mobile, les moyens précités de traitement de l'information étant conçus pour, à chaque utilisation de cette deuxième carte, vérifier l'existence d'une autorisation préalable donnée par le porteur du téléphone mobile ou envoyer un message au téléphone mobile demandant une acceptation ou un refus de ladite utilisation.

Le procédé et le système selon l'invention permettent de sécuriser les transactions effectuées au moyen de cartes de paiement sur des terminaux informatiques d'un type quelconque (terminaux de paiements électroniques, distributeurs automatiques de billets, paiements effectués sur le réseau Internet ou par téléphone, etc...).

Ce procédé et ce système permettent également, de façon générale, de sécuriser l'utilisation de cartes ou de (supports d'informations d'un type quelconque comportant des) moyens d'identification et/ou d'authentification, en informant leurs détenteurs de toute utilisation frauduleuse ou non conforme à des conditions prédéterminées et en leur permettant de s'opposer à cette utilisation.

L'invention sera mieux comprise et d'autres caractéristiques, détails et avantages de celle-ci apparaîtront plus clairement à la lecture de la description qui suit, faite à titre d'exemple en référence aux dessins annexés dans lesquels :

- la figure 1 représente schématiquement le système de sécurisation selon l'invention ;
- les figures 2 et 3 sont des organigrammes représentant les principales étapes du procédé selon l'invention.

On va décrire dans ce qui suit l'application de l'invention à la sécurisation de l'utilisation de cartes bancaires de paiement 10 d'un type classique (carte bleue, visa, eurocard, etc...) comprenant par exemple une bande magnétique et/ou des circuits intégrés formant support d'informations d'identification et d'authentification d'une carte et/ou de son titulaire.

Ces cartes 10 sont utilisables sur des terminaux informatiques tels que ceux représentés en 12 en figure 1 que l'on trouve actuellement dans la plupart

des magasins, points de vente, etc... et qui sont reliés à un réseau informatique bancaire 14 par l'intermédiaire du réseau téléphonique commuté public. Ces cartes sont également utilisables sur des distributeurs automatiques de billets tels que celui représenté en 16. Elles peuvent également être utilisées pour des transactions effectuées par téléphone ou sur le réseau Internet à partir d'un terminal informatique 18 du type PC : dans ce cas, l'acheteur communique le numéro de sa carte de paiement au vendeur qui lui-même émet un ordre de paiement par débit du compte bancaire de l'acheteur, cet ordre de paiement étant transmis au réseau bancaire 12 par le vendeur avec le numéro de la carte de paiement de l'acheteur.

Si les transactions effectuées au moyen d'une carte 10 sur un terminal 12 d'un point de vente ou sur un distributeur automatique de billets 16 nécessitent la connaissance du code confidentiel associé à la carte de paiement et offrent de ce fait une certaine sécurité, il n'en est pas de même actuellement lorsque ces cartes sont utilisées sur le réseau Internet puisqu'il suffit pour autoriser un paiement de communiquer un numéro de carte qui peut être intercepté par un tiers qui s'en servira ensuite frauduleusement.

L'invention propose d'assurer la sécurité de l'utilisation de ces cartes grâce à une association avec un réseau de radiotéléphonie, par exemple du type GSM ou autre.

Pour cela, l'invention prévoit d'associer chaque carte de paiement 10 à un radiotéléphone ou téléphone mobile 20 en enregistrant dans une base de données 22 un couple d'informations comprenant un identifiant de la carte de paiement 10 et un identifiant du téléphone mobile 20 et/ou de la personne abonnée à un réseau 24 de radiotéléphone et portant le téléphone mobile 20.

L'identifiant de la carte 10 peut comprendre son numéro 26, tel qu'il figure sur la carte, avec une information supplémentaire indiquant que la carte appartient au système selon l'invention. L'identifiant du radiotéléphone 20 ou de l'abonné correspondant peut être, soit le numéro d'appel du radiotéléphone 20, soit une information d'identification de l'abonné telle que IMSI (International Mobile Subscriber Identity) qui permet au réseau de radiotéléphonie 24 de

repérer un abonné de manière unique, cette information n'étant pas connue de l'abonné à qui il est seulement fourni le numéro d'appel de son radiotéléphone 20. Une base de données dans le réseau de radiotéléphonie 24 permet de faire la correspondance entre le numéro d'appel du radiotéléphone 20 et l'information d'identification de l'abonné, utilisée dans le réseau 24 pour la localisation de cet abonné.

L'invention prévoit également d'enregistrer, dans une base de données 28, des informations relatives aux terminaux sur lesquels peuvent être utilisés les cartes 10, ces informations comprenant un identifiant du terminal et son emplacement géographique.

L'identifiant du terminal est automatiquement fourni au réseau bancaire 14 à chaque utilisation d'une carte 10 sur ce terminal. Son emplacement peut éventuellement être connu lorsqu'il s'agit d'un terminal fixe tel qu'un distributeur automatique de billets 16, mais il est plus généralement déterminé à sa première utilisation à partir de la localisation du radiotéléphone 20 de la personne qui utilise sa carte 10 sur ce terminal, comme cela sera décrit plus en détail dans ce qui suit.

L'invention prévoit aussi une troisième base de données 30 dans laquelle sont enregistrées des informations relatives aux cartes 10 associées à des radiotéléphones 20, telles par exemple que la nature de cette carte, son état d'activation ou de désactivation, des conditions limites d'utilisation et des autorisations préalables d'utilisation.

Le système selon l'invention comprend un serveur informatique 32, permettant de mettre à jour et d'exploiter les informations contenues dans les bases de données 22, 28 et 30, des moyens de connexion 34 à un serveur 36 du réseau bancaire 14 et des moyens de connexion 38 à un serveur 40 du réseau de radiotéléphonie 24.

L'invention prévoit également d'utiliser la carte électronique ou carte d'abonnement qui équipe chaque radiotéléphone 20 (la carte SIM ou Subscriber Identity Module) qui permet à l'abonné d'avoir accès aux services du réseau 24 de radiotéléphonie et qui contient toutes les données concernant l'abonné et

notamment des moyens d'authentification et des informations relatives à l'abonnement, ce module comportant des circuits intégrés comprenant un microprocesseur et des mémoires du type ROM, EPROM et RAM. Selon l'invention, ces moyens sont programmés pour d'une part, authentifier la carte 10 associée au radiotéléphone 20 et, d'autre part, offrir à l'abonné un certain nombre de fonctions supplémentaires, telles notamment que des autorisations préalables d'utilisation de la carte 10, des fonctions d'activation et de désactivation de cette carte, et des fonctions d'acceptation et de refus d'une utilisation de la carte 10.

L'invention prévoit également d'associer deux cartes 10 ou plusieurs cartes à un même radiotéléphone 20, l'une de ces cartes étant détenues par le porteur du radiotéléphone, l'autre ou les autres cartes étant remises chacune à une personne différente. Dans ce cas, le moyen (module) d'identification d'abonné du radiotéléphone comprend des fonctions permettant au porteur du radiotéléphone d'autoriser préalablement des utilisations de ladite autre carte ou desdites autres cartes, avec fixation de conditions limites d'utilisation (notamment de plafonds de transaction), des fonctions d'activation et de désactivation de cette autre carte ou de ces autres cartes, et des fonctions d'acceptation et de refus des utilisations de cette autre carte ou de ces autres cartes.

Ces autres cartes peuvent par exemple être remises par un employeur à des employés, ou par des parents à leurs enfants, etc...

Le fonctionnement du système de sécurisation selon l'invention va maintenant être décrit en référence à la figure 2.

A chaque utilisation d'une carte 10 sur un terminal informatique 12, 16 ou 18, un certain nombre d'informations, telles que l'identifiant de la carte, l'identifiant du terminal et le montant de la transaction sont traitées par le serveur 36 du réseau bancaire 14. Lorsque l'identifiant de la carte 10 révèle son appartenance au système selon l'invention, les identifiants du terminal utilisé et de la carte 10 ainsi que le montant de la transaction sont transmis par le serveur 36 au serveur 32 du système selon l'invention (étape 44) qui, dans un premier

temps, va vérifier l'état d'activation ou de désactivation de la carte 10 (étape 46), cette information se trouvant dans sa base de données 30.

Le serveur 32 a également accès, dans sa base de données 22, à l'identifiant du radiotéléphone 20 ou d'abonné qui est associé à l'identifiant de la carte 10.

Si cette carte est activée, le serveur 32 envoie, à l'étape 48, une demande de localisation du radiotéléphone 20 au serveur 40 du réseau de radiotéléphonie 24.

Si le radiotéléphone 20 ne peut être localisé comme indiqué en 50 (il est par exemple éteint), le serveur 32 du système selon l'invention envoie au serveur 36 du réseau bancaire 14 un refus 52 de la transaction effectuée par la carte 10 sur le terminal 12, 16 ou 18.

Quand le radiotéléphone 20 est localisable, son emplacement approximatif est transmis par le serveur 40 du réseau de radiotéléphonie 24 au serveur 32 du système selon l'invention qui, dans sa base de données 28, a trouvé l'emplacement du terminal utilisé, cette information d'emplacement étant accessible à partir de l'identifiant du terminal transmis par le serveur 36.

Le serveur 32 effectue ensuite, comme indiqué en 54, une comparaison de l'emplacement du terminal 12 ou 16 et de l'emplacement localisé du radiotéléphone 20 et compare éventuellement le montant de la transaction effectuée avec la carte 10 à un plafond préenregistré dans sa base de données 30.

Si les emplacements du terminal 12 ou 16 et du radiotéléphone 20 correspondent et si le montant de la transaction est inférieur au plafond préenregistré, comme indiqué en 56, le serveur 32 envoie au serveur 36 du réseau bancaire une information d'acceptation de la transaction effectuée au moyen de la carte 10 sur le terminal 12 ou 16.

Lorsque l'emplacement du terminal enregistré dans la base de données 28 ne correspond pas à l'emplacement localisé du radiotéléphone 20 et/ou si le montant de la transaction est supérieur au plafond préenregistré dans la base de données 30, le serveur 32 appelle le radiotéléphone 20, par l'intermédiaire du

serveur 40 et du réseau de radiotéléphonie 24, pour demander au porteur du radiotéléphone de valider la transaction, comme indiqué en 60 (en mode data ou vocal, suivant le risque par exemple). Si le porteur du radiotéléphone 20 valide la transaction comme indiqué en 62, le serveur 32 du système selon l'invention envoie au serveur 36 du réseau bancaire 14 une acceptation de la transaction, comme indiqué en 58.

Si le porteur du radiotéléphone 20 ne valide pas la transaction comme indiqué en 64, le serveur 32 du système selon l'invention envoie un refus au serveur 36 du réseau bancaire 14, comme indiqué en 66.

Si le terminal utilisé 12, 16, 18 est inconnu du système selon l'invention (son identifiant et son emplacement n'ont pas été enregistrés dans la base de données 28), le serveur 32 enregistre dans cette base de données l'emplacement localisé du radiotéléphone 20 en l'associant à l'identifiant du terminal. Il passe ensuite à l'étape précitée 60 d'appel du radiotéléphone 20, pour demander une validation ou un refus de la transaction par le porteur du radiotéléphone.

Lorsque le serveur 32 du système selon l'invention constate, à l'issue de l'étape 46, que la carte 10 est désactivée comme indiqué en 70, il passe à l'étape 60 d'appel du radiotéléphone 20 pour demander une validation ou un refus de la transaction.

Ces opérations de validation ou de refus d'une transaction par le porteur du radiotéléphone sont effectuées à l'aide des touches de fonction du radiotéléphone, sélectionnées à partir d'un menu enregistré dans les mémoires du moyen (module) d'identification d'abonné. De plus, les informations préenregistrées dans ce module permettent d'authentifier les transactions effectuées avec une carte 10. Par exemple, lorsque le téléphone mobile 20 a été localisé et que cette localisation permet au serveur 32 d'accepter une transaction comme indiqué aux étapes 54 et 56, les informations contenues dans le module d'identification d'abonné du radiotéléphone 20 permettent au serveur 32 d'authentifier la transaction effectuée avec la carte 10. Les demandes de validation prévues à l'étape 60 peuvent comprendre la frappe, sur les touches du

radiotéléphone 20, du code confidentiel associé à la carte 10. Dans ce cas, la vérification du code tapé sur le radiotéléphone 20 et du code confidentiel de la carte est effectuée par le module d'identification d'abonné du radiotéléphone et conditionne l'envoi par le serveur 32 d'une acceptation ou d'un refus de la transaction.

C'est également au moyen des touches de fonction du radiotéléphone et d'un menu enregistré dans le module d'identification d'abonné, qu'une personne peut signaler au serveur 32 l'activation ou la désactivation de sa carte de paiement 10, ou bien une autorisation préalable d'une utilisation prévue de cette carte avec fixation d'un montant maximum de paiement.

Ces fonctions permettent au titulaire d'une carte 10 de l'utiliser pour un paiement par téléphone ou sur Internet et de la prêter à un tiers qui ne pourra s'en servir qu'avec l'accord du titulaire puisque le serveur 32 qui constate des différences d'emplacement d'un terminal de paiement et du radiotéléphone 20 ou le dépassement d'un montant autorisé va demander une validation de la transaction au porteur du radiotéléphone.

Ces fonctions permettent également au porteur du radiotéléphone 20 de contrôler l'utilisation d'une ou de plusieurs autres cartes 10 qui ont été confiées à d'autres personnes, comme représenté schématiquement en figure 3.

Dans ce cas, la carte détenue par le porteur du radiotéléphone 20 est considérée comme une carte maître tandis que la ou les autres cartes de paiement sont considérées comme des cartes esclaves.

La carte maître peut être utilisée normalement par son détenteur, comme déjà décrit en référence à la figure 2 : le serveur 32 après avoir vérifié que la carte est activée et qu'il s'agit d'une carte maître comme indiqué en 72, passe à l'étape 48 de demande de localisation du radiotéléphone.

Lorsque le serveur 32, après avoir vérifié que la carte utilisée est bien activée, constate qu'il s'agit d'une carte esclave comme indiqué en 74 (cette information se trouve dans sa base de données 30) et compare ensuite le montant de la transaction effectuée avec cette carte à un plafond préenregistré dans sa base de données 30, comme indiqué en 76. Si le montant est supérieur

au plafond enregistré, le serveur 32 appelle le téléphone mobile 20 pour demander une validation de la transaction (c'est l'étape 60 de la figure 2). Si le montant de la transaction est inférieur au plafond enregistré, le serveur 32 accepte la transaction et envoie une information correspondante au serveur 36 du réseau bancaire 14 (étape 58 de la figure 2).

Exemples d'utilisation :

Le porteur du radiotéléphone 20 effectue des achats avec sa carte de paiement 10 dans un centre commercial. Il quitte ensuite le centre commercial. Plus tard, son radiotéléphone sonne et il lit sur l'écran d'affichage le message suivant : "1500 francs au magasin XYZ - voulez-vous valider ?". Il vérifie dans son porte-carte, sa carte de paiement 10 ne s'y trouve pas. Il répond "NON". Il appuie ensuite sur la touche "MENU" de son radiotéléphone puis sélectionne "CARTE DE PAIEMENT" et la fonction "DESACTIVATION". Le serveur 32 du système selon l'invention refuse alors toute transaction effectuée au moyen de la carte.

- Le porteur du radiotéléphone 20 prête sa carte de paiement à sa fille qui souhaite faire un achat d'environ 800 francs. Un peu plus tard, son radiotéléphone sonne et il lit sur l'écran d'affichage : "900 francs chez XYZ, voulez-vous valider ?". Il appuie sur la touche "VALIDATION" en pensant que sa fille a un peu dépassé le montant prévu.

- Le porteur du radiotéléphone 20 souhaite faire quelques achats sur le réseau Internet en utilisant sa carte de paiement. Il appuie sur la touche "MENU" de son radiotéléphone, puis sélectionne "CARTE DE PAIEMENT", choisit la fonction "PRE-AUTORISATION" et frappe ensuite un montant de 1200 francs. Il achète ensuite sur le réseau Internet quelques articles pour un montant de 340 francs, en tapant le numéro de sa carte de paiement sur le clavier de son micro-ordinateur connecté au réseau Internet. Il n'est pas appelé sur son radiotéléphone pour une demande de validation.

Un peu plus tard, il utilise à nouveau sa carte de paiement pour acheter des objets sur un autre site Internet. Le montant de la transaction est d'environ 1000 francs. Il frappe son numéro de carte sur le clavier de son micro-ordinateur.

Avant l'acceptation de son paiement par le vendeur, son radiotéléphone sonne pour lui demander de valider la transaction (il a dépassé le montant préautorisé).

- En arrivant à son bureau, le porteur du radiotéléphone 20 s'aperçoit qu'il n'a pas son porte-carte. Il appuie sur la touche "MENU" de son radiotéléphone puis sélectionne "CARTE DE PAIEMENT" et choisit la fonction "DESACTIVATION". Rentré à son domicile, il retrouve son porte-carte. Avec son radiotéléphone, il réactive sa carte de paiement.

- Le porteur du radiotéléphone 20 a confié à un employé une carte de paiement "esclave" pour lui permettre de payer ses frais de déplacement et de séjour en province pendant quelques jours. Au moyen des touches de fonction de son radiotéléphone, il fait enregistrer dans la base de données 30 du système selon l'invention une autorisation de 1500 francs valable pendant trois jours sur la carte de paiement confiée à l'employé.

- Le porteur du radiotéléphone 20 a effectué il y a quelque temps des achats chez un commerçant, en utilisant sa carte de paiement 10. Dans l'intervalle, le commerçant a changé d'adresse et se trouve maintenant dans un autre quartier de la ville. Lorsqu'un autre porteur d'un radiotéléphone de type 20 se rend à nouveau chez ce commerçant et qu'il utilise sa carte de paiement sur le terminal 12 du commerçant, le serveur 32 du système selon l'invention constate que l'emplacement localisé du radiotéléphone ne correspond pas avec l'emplacement du terminal 12 enregistré dans sa banque de données 28. Il appelle le radiotéléphone 20 pour demander validation de la transaction et enregistre l'emplacement localisé du radiotéléphone comme nouvel emplacement du terminal 12 dans sa base de données 28.

De façon générale, le serveur 32 du système selon l'invention peut vérifier, sans appeler le radiotéléphone 20, la cohérence entre le numéro de la carte de paiement du porteur et les identifiants enregistrés dans le module d'identification d'abonné équipant le radiotéléphone.

Au niveau suivant de vérification, le serveur 32 appelle le radiotéléphone 20 et demande par message sur l'écran d'affichage une validation de la transaction en cours.

Au niveau suivant de vérification, le serveur 32 appelle le radiotéléphone 20 et demande sur l'écran d'affichage la saisie, au moyen des touches du radiotéléphone, du code confidentiel associé à la carte de paiement.

A un niveau ultérieur de vérification, le serveur 32 appelle le radiotéléphone 20 et demande à parler au porteur pour l'informer sur le risque de la transaction tout en lui demandant de saisir le code confidentiel de sa carte de paiement.

Au dernier niveau de vérification, le serveur 32 envoie au serveur 36 du réseau bancaire un refus de transaction.

L'invention s'applique, non seulement à l'exemple qui a été décrit et représenté, mais aussi à la sécurisation de toute utilisation de cartes ou d'autres (supports d'informations comprenant des) moyens d'identification et/ou d'authentification, tels par exemple que des cartes de santé, des cartes d'accès à des zones protégées, des porte-monnaies électroniques, etc. et à la sécurisation d'accès et de loging à des réseaux informatiques (de type intranet par exemple) ou à des fichiers privés de données, etc.

REVENDICATIONS

1. Procédé de sécurisation de l'utilisation de cartes et autres (supports comportant des) moyens d'identification et/ou d'authentification, en particulier de cartes bancaires de paiement, caractérisé en ce qu'il consiste :

- à associer chaque carte (10) précitée à un radiotéléphone (20) équipé d'un moyen (module) d'identification d'abonné à circuits intégrés et à enregistrer dans une base de données (22) un couple d'informations comprenant un identifiant de la carte (10) et un identifiant du radiotéléphone (20) ou de l'abonné,

- et, à chaque utilisation de la carte (10) sur un terminal informatique (12, 16) dont l'emplacement est connu, à localiser au moyen du réseau de radiotéléphonie (24) le radiotéléphone (20) associé à cette carte, à comparer l'emplacement du terminal informatique (12, 16) et l'emplacement localisé du radiotéléphone (20) et, en fonction du résultat de cette comparaison, à valider l'utilisation de la carte (10) sur le terminal informatique (12, 16) ou à appeler le radiotéléphone (20) pour acceptation ou refus par son porteur de l'utilisation de la carte (10) sur le terminal informatique (12, 16).

2. Procédé selon la revendication 1, caractérisé en ce qu'il consiste, à l'utilisation d'une carte précitée (10) sur un terminal (12, 16, 18) dont l'emplacement est inconnu, à enregistrer un identifiant de ce terminal et son emplacement déterminé par la localisation du radiotéléphone (20) associé à la carte (10), et à constituer une base de données (28) contenant les identifiants et les emplacements des terminaux informatiques utilisés au moyen des cartes (10) précitées.

3. Procédé selon la revendication 2, caractérisé en ce qu'il consiste, lors d'une utilisation ultérieure du même terminal avec par exemple une autre carte, à localiser le radiotéléphone (20) associé à cette carte, à vérifier la concordance entre l'emplacement du radiotéléphone et celui du terminal enregistré précédemment dans la base de données (28) et, en cas de discordance entre ces emplacements, à appeler le radiotéléphone (20) pour acceptation ou refus de l'utilisation de ladite carte sur ce terminal.

4. Procédé selon l'une des revendications précédentes, caractérisé en ce que l'identifiant d'une carte (10) précitée associée à un radiotéléphone (20) permet de la distinguer d'une carte (10) non associée à un radiotéléphone.

5. Procédé selon l'une des revendications précédentes, caractérisé en ce qu'il consiste à enregistrer dans les circuits intégrés du moyen (module) d'identification d'abonné équipant le radiotéléphone (20), un logiciel comprenant des moyens d'authentification de la carte (10) associée à ce radiotéléphone.

6. Procédé selon l'une des revendications précédentes, caractérisé en ce qu'il consiste à enregistrer dans les circuits intégrés du moyen (module) d'identification d'abonné équipant le radiotéléphone (20) un logiciel comprenant des fonctions d'autorisation préalable d'utilisation de la carte associée (10), d'activation et de désactivation de cette carte, et d'acceptation ou de refus d'utilisation de la carte (10) précitée.

7. Procédé selon l'une des revendications précédentes, caractérisé en ce qu'il consiste à associer au moins deux cartes (10) précitées à un radiotéléphone (20) équipé d'un moyen (module) d'identification d'abonné, l'une des cartes (10) étant utilisable par le porteur du radiotéléphone et l'autre par une autre personne, et à soumettre chaque utilisation de cette autre carte (10) à une autorisation préalable, à une acceptation ou à un refus par le porteur du radiotéléphone (20).

8. Procédé selon l'une des revendications précédentes, caractérisé en ce qu'il consiste à enregistrer dans une base de données (30) des informations associées à chaque carte (10) et concernant sa nature, son état d'activation ou de désactivation, des conditions limites d'utilisation et des autorisations préalables d'utilisation.

9. Système de sécurisation de l'utilisation de cartes et autres (supports munis de) moyens d'identification et/ou d'authentification, en particulier de cartes bancaires de paiement, caractérisé en ce qu'il comprend :

- une première base de données (22) dans laquelle sont enregistrés des identifiants de radiotéléphones ou d'abonnés à un réseau de radiotéléphonie (24) et des identifiants de cartes précitées (10) détenues par les abonnés ou par des

personnes autorisées par les abonnés, chaque identifiant de carte (10) étant associé à un identifiant de radiotéléphone (20) ou d'abonné,

- une deuxième base de données (28) dans laquelle sont enregistrés des identifiants et des emplacements de terminaux informatiques sur lesquels les cartes (10) précitées sont utilisables,

- des moyens (32) de traitement de l'information pour la constitution, la mise à jour et la gestion desdites bases de données,

- des moyens (34, 38) de connexion de ces moyens (32) de l'information à un serveur (36) d'un système existant de traitement de l'utilisation des cartes (10) précitées sur des terminaux informatiques et à un serveur (40) d'un réseau de radiotéléphonie (24) sur lequel les radiotéléphones (20) sont utilisables,

- lesdits moyens (32) de traitement de l'information étant conçus pour, à chaque utilisation d'une carte (10) précitée sur un terminal informatique (12, 16, 18), trouver dans la première base de données (22) l'identifiant de radiotéléphone ou d'abonné qui est associé à l'identifiant de la carte (10) utilisée, transmettre au serveur (40) du réseau de radiotéléphonie une demande de localisation du radiotéléphone (20) associé à ladite carte (10), trouver dans la deuxième base de données (28) l'emplacement du terminal informatique utilisé par ladite carte (10), comparer cet emplacement avec l'emplacement localisé du radiotéléphone (20) et, en fonction du résultat de cette comparaison, valider l'utilisation de la carte (10) sur le terminal (12, 16, 18) ou envoyer un message au radiotéléphone (20) demandant une acceptation ou un refus, par le porteur du radiotéléphone (20), de l'utilisation de la carte (10) sur le terminal informatique précité.

10. Système selon la revendication 9, caractérisé en ce que l'identifiant d'une carte (10) associée à un radiotéléphone (20) permet de la distinguer d'une carte (10) non associée à un radiotéléphone.

11. Système selon la revendication 9 ou 10, caractérisé en ce que le moyen (module) d'identification d'abonné équipant le radiotéléphone (20) comprend des moyens d'authentification de la carte (10) précitée.

12. Système selon l'une des revendications 9 à 11, caractérisé en ce que le moyen (module) d'identification d'abonné équipant le radiotéléphone (20) comprend des moyens d'autorisation préalable d'au moins une utilisation de la carte (10) associée, des moyens d'activation et de désactivation de cette carte, et des moyens d'acceptation et de refus de l'utilisation de cette carte (10) sur un terminal informatique précité.

13. Système selon l'une des revendications 9 à 12, caractérisé en ce qu'il comprend une troisième base de données (30) dans laquelle sont enregistrées des informations relatives à chaque carte associée à un radiotéléphone (20), ces informations concernant sa nature, son état d'activation ou de désactivation, des conditions limites d'utilisation et des autorisations préalables d'utilisation.

14. Système selon l'une des revendications 9 à 13, caractérisé en ce qu'au moins une deuxième carte (10) est associée à un radiotéléphone (20) déjà associé à une première carte (10) et est utilisable par une autre personne que le porteur du radiotéléphone (20), les moyens précités (32) de traitement de l'information étant conçus pour, à chaque utilisation de cette deuxième carte, vérifier l'existence d'une autorisation préalable donnée par le porteur du radiotéléphone (20) ou envoyer un message au téléphone mobile (20) demandant une acceptation ou un refus de cette utilisation de la deuxième carte (10).

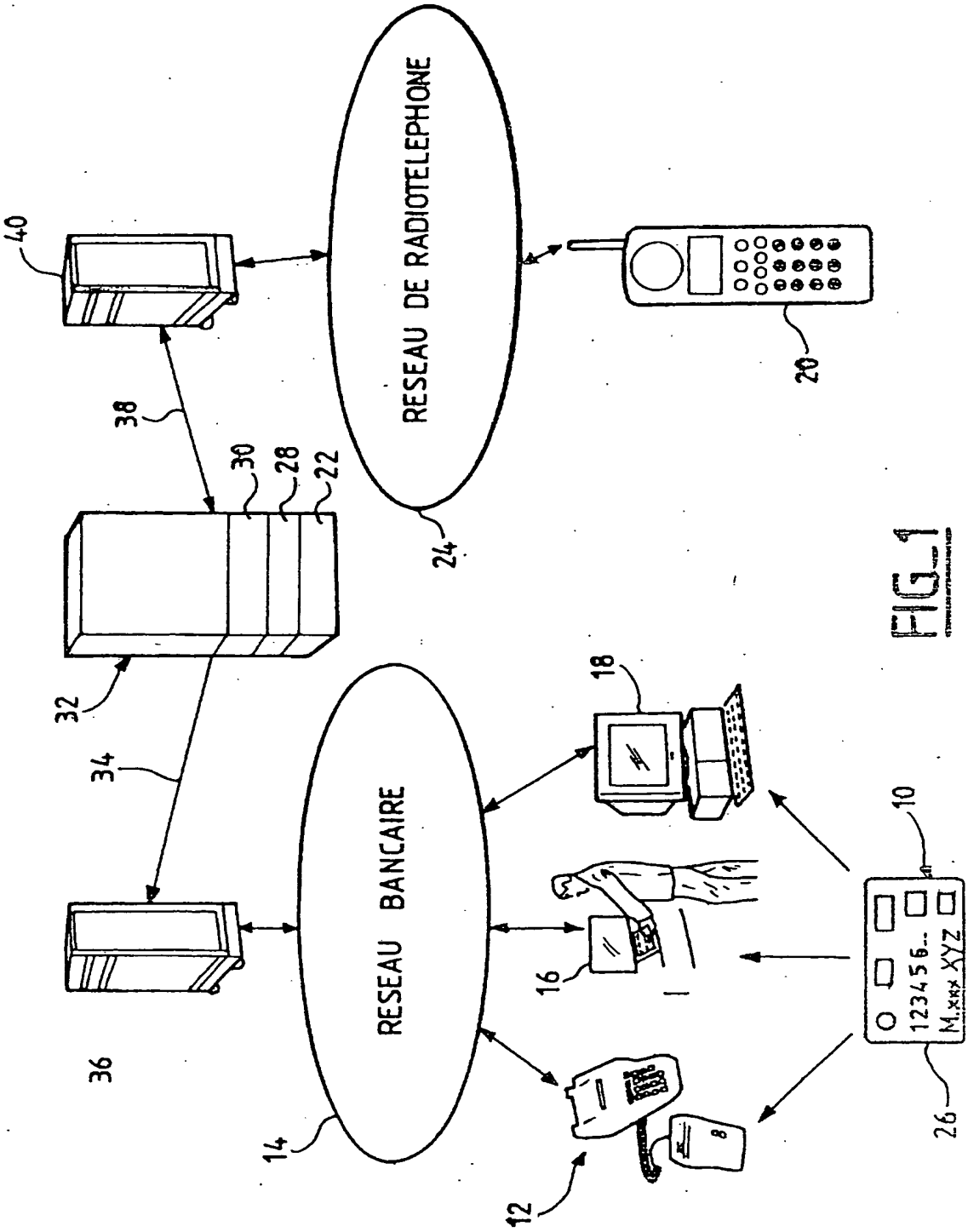

RESEAU DE RADIOTELEPHONE
RESEAU BANCAIRE
40
38
30
28
22
32
34
36
24
20
18
10
16
12
14
26
123456..
M.XXX XYZ

FIG_1

FIG_2

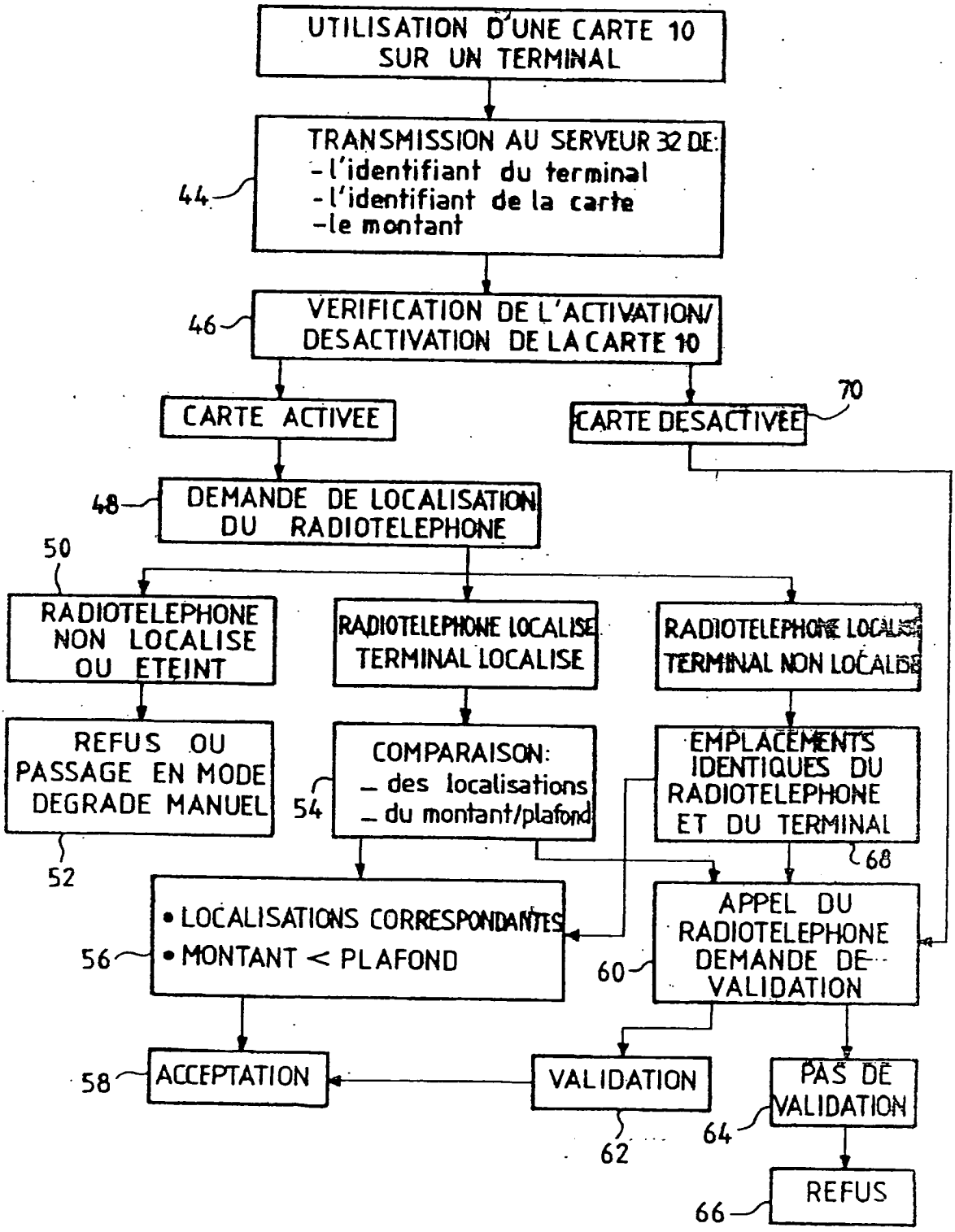
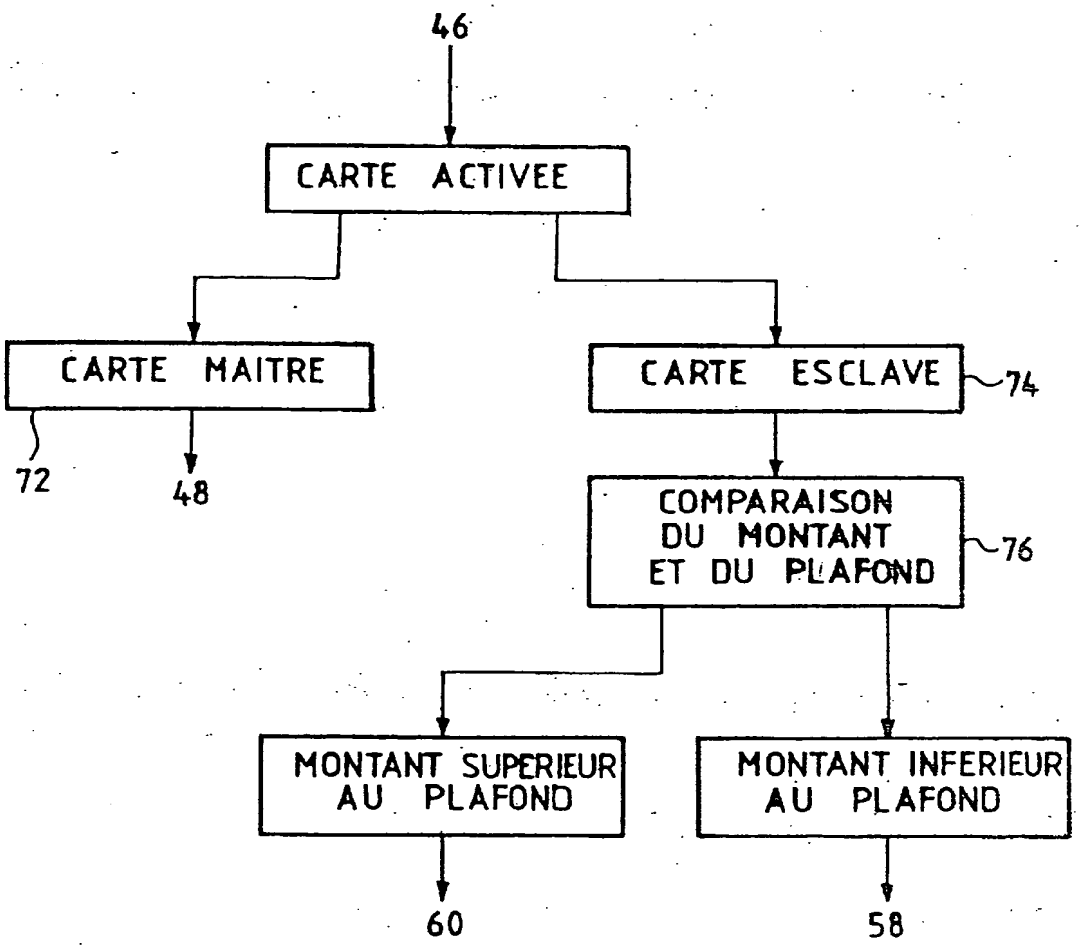

UTILISATION D'UNE CARTE 10 SUR UN TERMINAL
TRANSMISSION AU SERVEUR 32 DE:
- l'identifiant du terminal
- l'identifiant de la carte
- le montant
44
VERIFICATION DE L'ACTIVATION/ DESACTIVATION DE LA CARTE 10
46
CARTE ACTIVEE
CARTE DESACTIVEE
70
DEMANDE DE LOCALISATION DU RADIOTELEPHONE
48
50
RADIOTELEPHONE NON LOCALISE OU ETEINT
RADIOTELEPHONE LOCALISE TERMINAL LOCALISE
RADIOTELEPHONE LOCALISE TERMINAL NON LOCALISE
REFUS OU PASSAGE EN MODE DEGRADE MANUEL
52
COMPARAISON:
- des localisations
- du montant/plafond
54
EMPLACEMENTS IDENTIQUES DU RADIOTELEPHONE ET DU TERMINAL
68
• LOCALISATIONS CORRESPONDANTES
• MONTANT < PLAFOND
56
APPEL DU RADIOTELEPHONE DEMANDE DE VALIDATION
60
ACCEPTATION
58
VALIDATION
62
PAS DE VALIDATION
64
REFUS
66

FIG_3


46
CARTE ACTIVEE
CARTE MAITRE
CARTE ESCLAVE
74
72
48
COMPARAISON DU MONTANT ET DU PLAFOND
76
MONTANT SUPERIEUR AU PLAFOND
MONTANT INFERIEUR AU PLAFOND
60
58

REPUBLIQUE FRANÇAISE

2792143

INSTITUT NATIONAL
de la
PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRELIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

N° d'enregistrement national

FA 571271
FR 9904537

DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendications concernées de la demande examinée
X	WO 98 06214 A (BOCK ROBERT RICHARD ;JOAO RAYMOND ANTHONY (US)) 12 février 1998 (1998-02-12)	1,7,8
A	* page 6 - page 7 * * page 8, alinéa 3 - page 9, alinéa 1 * * page 10 * * page 12, alinéa 3 - page 13, alinéa 2 * * page 17, alinéa 3 - alinéa 5 * * page 27 * * page 28, ligne 36 - page 29, ligne 2 * * revendications 1-3,10,16 *	2,3,6,9, 11-14
Y	WO 98 47116 A (ERICSSON TELEFON AB L M) 22 octobre 1998 (1998-10-22)	1,4,9
A	* page 3, ligne 24 - page 4, ligne 16 * * revendications 1-6 *	2,3,8,13
Y	WO 99 14711 A (ANDRASEV AKOS) 25 mars 1999 (1999-03-25)	1,4,9
A	* page 6, ligne 20 - page 7, ligne 13 * * page 12, ligne 33 - page 13, ligne 7 * * page 18, ligne 22 - page 19, ligne 6 * * revendication 5 *	7,8,10, 11,13,14
A	US 5 615 110 A (WONG KAM-FU) 25 mars 1997 (1997-03-25) * colonne 2, ligne 52 - colonne 3, ligne 35 * * revendications 17-21 *	1,7-9, 11,13,14

DOMAINES TECHNIQUES RECHERCHES (Int.CL.7)

G07F

1

Date d'achèvement de la recherche	Examinateur
20 janvier 2000	Wolles, B

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 03.82 (P04C13)